



August 5, 2014

Comments Regarding Big Data and Consumer Privacy in the Internet Economy  
Docket No. 140514424-4424-01

In support of our more than 30,000 individual app developer members and more than 150 corporate members, the Application Developers Alliance (“Alliance”) writes to share its views regarding consumer privacy concerns associated with so-called “big data”.

Alliance members deliver the benefits of data to our users and also protect the privacy of users’ data. These are not mutually exclusive; app developers accomplish both. Alliance members understand that consumer enjoyment is irrelevant if trust is lacking, and that trust is a fundamental requirement of business success. If consumers decide that an app cannot be trusted with their data, the app will not succeed.

The benefits of data have become extraordinary because the amount of data collected is vast and analysis tools are more powerful. Notwithstanding that increasing amounts of data are being collected and analyzed, there is very little new about so-called “big data” except that collection and analysis are easier. The Alliance believes that these advances do not independently justify reconsideration of traditional data policy. Instead, government should continue to focus attention on known and foreseeable risks of data misuse and to promote multistakeholder consensus-based processes that address these risks. Government should encourage industry implementation of consensus-based agreements by legislating enforcement safe harbors for companies that voluntarily provide additional safeguards against data misuse.

While Alliance members are optimistic about the power of data to positively transform our world, they appreciate the potential for data misuse. There are more participants in data driven industries relying on more data to provide more services, and they are focused on providing a positive impact for consumers. As with any industry, misuse may occur, so we welcome government scrutiny into whether such misuse exists and how to address any examples. The nature of the data industries, however, has not changed, and the principles of oversight and enforcement should not change merely because the industry is larger.

Though the National Telecommunications and Information Administration (“NTIA”) raises many relevant questions, these Comments focus on three points that app developers believe are critically important. The Alliance’s Comments:

1. Discourage data collection limitations but endorse and describe a workable responsible use framework;
2. Endorse legislative safe harbors to encourage adoption of targeted solutions to discrete data misuses; and,
3. Express concerns regarding default privacy preference profiles.

## **I. Data Collection Is Increasing; Analysis is Faster; and Limiting Either Collection or Analysis Will Rob Consumers of Their Benefits**

More data is collected and analyzed now because data powers personalized opportunities that consumers desire. For example, consumers enjoy context-specific offerings at places and times they can be used; apps that quantify data from our bodies and help improve our health; and, relevant advertising that offers desirable savings opportunities. Similarly, consumers enjoy the benefits of wearable devices that improve health and sensors that collect data in cars, on roads and even in home appliances.

Our ability to understand and benefit from data is also improving due to analytics advancements. Cheaper data storage and faster processors support these advances, but the driver is individuals' desire for knowledge that improves lives. The Alliance believes that policymakers should embrace the growing promise of data analytics to solve previously intractable problems and benefit underserved communities.

Some fear the growing amounts of data collection and analysis, and propose limits. These proposals should be rejected because collection limits would limit the benefits of data innovation. For example:

- Limiting collection of financial transaction patterns, including geolocation patterns, would inhibit fraud-prevention techniques that facilitate credit cards, mobile payments and mobile banking apps.
- Limiting collection of biometric data would inhibit health quality monitoring apps.
- Limiting collection by mobile road sensors would inhibit traffic jam avoiding apps.

Some proponents of collection limits cite the Fair Information Practice Principles ("FIPPs") as justification, but this approach undervalues consumer and societal benefits produced by data-based offerings. The FIPPs are important aspirational principles that advance privacy thinking and provide a framework for data-related decision making, but they are not the only relevant factors. Policy must carefully balance conceptual benefits of privacy with actual benefits of new products and services that rely on the availability and utility of data.

## **II. Data Misuses Are Foreseeable but Do Not Justify Data Collection or Analysis Limitations**

The Alliance acknowledges that consumer data misuses may occur that cause harm to consumers, their family members and neighbors. For example:

- Data can be misused to justify an otherwise unlawful decision, such as relying on accurate address data to justify redlining.
- Data can be lawfully collected for one purpose but unlawfully repurposed for unrelated (and potentially harmful) uses.
- Incorrect data can lead to significantly harmful decisions, e.g., regarding financial or educational opportunities.

None of these scenarios, however, justifies a government policy of limiting data collection or any types of data analyses or applications. These misuses may, however, justify targeted solutions to minimize the likelihood of occurrence and the associated harm. These solutions are discussed in more detail below.

### **III. The Existing Notice-and-Consent and Data Collection Limitation Model Should Be Replaced with a Responsible Data Use Framework that Promotes Targeted, Consensus-Based Solutions and Protects Early-Adopters**

Today's notice-and-consent model of data collection is a failure for consumers. It forces businesses to hire lawyers to write lengthy notices filled with legalese, which nobody reads. This results in consumers receiving proper legal notice but not actual notice. It creates opportunities for class action lawyers and government enforcement that thrive on technical deviations from written policy without considering whether the deviation was material or harmed consumers. Further, it inhibits data and privacy innovation because companies' lawyers counsel avoiding risk associated with change.

The Alliance supports a new approach to data collection, usage and management—a responsible data use framework that is a foundation for contextual consensus-based solutions. By enabling contextual consensus solutions, this framework promotes more innovation and permits more nuances than will a broad legislative mandate. This approach should account for whether the data use is within consumer expectations as well as whether it is harmful to consumers. Thus, the Alliance believes that this structure would benefit consumers and developers.

A framework that allows society to maximize the benefits of data will both deter data misuse through targeted solutions to targeted problems and include safeguards that permit corporations to innovate with consumer data without fear of crippling legal risk. This balance requires time and commitment by all stakeholders, but the results for all parties will be improvements compared to the current situation and perpetual legislative stalemate.

The 2012-2013 NTIA multistakeholder discussions about mobile app privacy and transparency are a model for additional targeted, consensus-based solutions. A wide initial gulf between industry and privacy advocates narrowed over time, and targeted solutions were developed that attracted broad-based support and justified corporate investment in privacy innovation.

The Alliance would be pleased to participate in additional discussions that focus on difficult use cases, for example, relating to genetic data. These are very important discussions for employees and potential employees, and for employers, insurance companies (including labor union and employer sponsors) and the app developers they work with.

When voluntary, consensus-based solutions are developed, government can promote them by enacting safe harbor legislation that shields corporate early adopters from enforcement and class action risk. This will benefit consumers by more quickly bringing broadly supported, discrete solutions to the public. Currently, without safe harbor, many companies are reticent about innovating on privacy due to liability concerns.

#### **IV. Default Privacy Settings Are Inconsistent with Consumers' Dynamic Privacy Preferences**

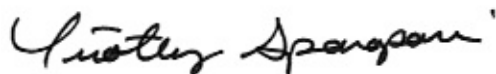
Proponents of mandatory default privacy settings assume that companies are not being transparent, that consumers do not understand or appreciate the importance of their data choices, or both. The Alliance believes that these assumptions are faulty. More important, however, is that policymakers and stakeholders can improve commercial transparency and consumer education, and thereby eliminate the need for mandatory default privacy settings.

Consumers are increasingly savvy about the benefits and potential risks of data collection and usage. Consumers' attitudes and requirements for privacy vary, and are context-specific. In contrast, default privacy settings lock consumers into binary privacy choices that require sharing all or none of their data. Static privacy profiles that "travel with data" and signal to business how to handle a consumer's data are not contextual and are overly simplistic.

Similarly, regulators should rely on companies and institutions to handle consumers' data responsibly and respectfully. Policies that mandate default privacy rules will squelch innovation and discourage companies from building products and services that offer customized options for individuals. Companies understand the risks of misusing data and work hard to keep consumer trust. Companies also work hard to provide consumers personalized offerings, and they need the option of working directly with consumers to develop and expand those offerings that people enjoy.

#### **Conclusion**

In conclusion, the Alliance urges policy makers to avoid confusion associated with so-called "big data". Policy makers should work with industry and stakeholders to identify and address the harms caused by data misuse through targeted solutions to defined problems. The government can encourage companies to initiate additional privacy protective measures by creating legal safe harbors for privacy-enhancing features and practices. The government should also premise policies on trusting that savvy consumers know what they want and that responsible companies will satisfy those demands and provide commensurate privacy and consumer protections.



Tim Sparapani  
Vice President, Policy, Law & Government Affairs  
Application Developers Alliance